Portals Rollout
Configuration Management Plan

Author: Brent W. Urcheck

Project Information

Executive Sponsor:	Jennifer Douglas / Steve Hawald / John Reeves
Project:	Portal Rollout
Project Manager:	Constance Davis / Jacqueline Dufort
Configuration Management Lead:	Brent W. Urcheck

Document History

Author	Date	Version	Description
Brent Urcheck	1/29/02	1.0	Portals Configuration Management Plan
Brent Urcheck	1/30/02	2.0	Revisions
Brent Urcheck	1/31/02	3.0	Revisions
Brent Urcheck	2/1/02	4.0	Revisions
Brent Urcheck	2/1/02	5.0	Revisions
Brent Urcheck	2/28/02	6.0	Revisions based on IV&V Feedback
Brent Urcheck	3/1/02	7.0	Revisions based on IV&V Feedback

Table of Contents

1.1 Purpose and Scope

Configuration Management (CM) refers to the processes, tools, and resources required to ensure consistency and integrity between documentation and configuration items and their environment as they change over time. Configuration management includes version control and change control. Version control includes tracking the changes made to documentation and application code and in the case of application code, an explanation as to why the changes were made. This is discussed in the configuration management activities section. Change control ensures that changes made are necessary and within the scope of the project. This is discussed in the configuration control section.

The purpose of this configuration management plan is to identify CM requirements, establish methodology for generating configuration items, control software and documentation changes, as well as to provide the Portals Rollout team with a framework from which configuration management processes will be established, maintained, and followed throughout the project life cycle and to. This framework will include:

- Roles and responsibilities required within the configuration management plan
- Steps required to version files
- The use of Microsoft Visual SourceSafe as a configuration management tool
- The use of ClearQuest as the modification requests and defect tracking tool

Electronic file configuration management is required to keep files synchronized with each other and the project as a whole. This configuration management process applies to all files (Word, Excel, PowerPoint, Project, etc.) created as a part of the project, whether as a deliverable to be given to the client or as an internal project working paper.

1.2 Organization, Responsibilities and Resources

This section details the authority and the specific responsibilities for configuration management throughout the project life cycle and identifies the specific resources necessary to perform effectively.

The Portals Rollout configuration management team will be composed of a configuration management lead, system test manager, performance test manager, tester(s), and developers.

1.2.1 Configuration Management Lead

The configuration management lead is responsible for interacting with the development teams to ensure all controlled items are checked in and out of code repository and any changes are tracked. For the purpose of the Portals design, the configuration management lead's responsibilities include:

- Managing the workflow of the development team, including assignment of modification requests
- Modification, logging, and closing of modification request tickets
- Accumulation and coordination of developer code changes in the development environment
- Transferring updated code to the development and testing environments
- Configuration Management of all deliverables

1.2.2 System Test Manager

The system test manager is responsible for planning and leading the testing effort for iterations that compose the Portals Rollout development approach. The specific responsibilities include:

- Creating detail test plans
- Monitoring resolution to noted defects
- Deciding to suspend or resume testing based on outstanding defects/issues
- Providing status to the Technical Project Lead and Configuration Management Lead
- Leading and participating in the testing process

1.2.3 Performance Test Manager

The performance test manager is responsible for planning, leading, and performing testing related to system and interface testing as well as testing related to performance and stress testing. The specific responsibilities include:

- Creating detail test plans relating to system and performance testing
- Monitoring, reporting, and acting upon testing results
- Coordination of modification requests resulting from testing with the configuration management lead
- Leading and executing testing related to performance

1.2.4 Developer (Development Team)

The developers are responsible for designing, documenting, building and unit testing all tasks assigned to them by the development team lead. These tasks may include creating source code, preparing unit test data, completing unit tests and code reviews. The developer is also responsible for addressing any defects or modification requests assigned to them during the testing stages. For the purposes of this design, developer responsibilities include:

- Executing unit testing
- Checking files in and out of the version control tool
- Participating in design and code reviews
- Implementing defect fixes and change requests
- Following project guidelines when using the configuration management tools

1.2.5 Tester(s)

The tester is responsible for planning and leading the testing effort. The tester will work with the development team lead to develop the test plan. These responsibilities include:

- Follow detailed test plans provided by the System Test Manager
- Execute test cases
- Monitoring resolution to noted defects and regression testing fixes to modification requests
- Provide status of testing progress to the System Test Manager and the Technical Project lead

1.2.6 System Security Officer (SSO)

A SSO is an individual formally designated to be responsible for the day-to-day security operations of a system. The primary function of a SSO is to implement the Department's ITSP (Information Technology Security Policy) as it applies to the system and the information that it handles or stores. The SSO shall work in close coordination with the Portals Rollout Project Manager. Specific SSO duties include, but are not limited to:

- Conduct a security review of all change requests and approving all changes from a security perspective
- Participates in assessing risk
- Implementing IT security for the assigned system
- Directly involved in configuration management processes for their assigned system

1.2.7 Change Control Group

The change control group evaluates requirements as they are identified to determine if the requirement is out of scope, in scope, or out of scope but should be included in the current project.

Role	Resource
Configuration Management Lead	Brent Urcheck
System Test Manager	Erick Middleton
Performance Test Manager	Mathew Wilson
Developer (Development Team)	Chris Lawson, Aimee Byrd
Tester(s)	Erick Middleton, Teale Taggart, Anne Jensen
Change Control Group	Steve Allison, Jacqueline Dufort, Brent Urcheck, Erick Middleton, Matthew Wilson, Philip Norton, Michael Page, Robert Lawrence, Johan Bos-Beijer, Francis Tang

1.3 Configuration Management Activities

1.3.1 Electronic File Configuration Management

Electronic file Configuration Management is required to keep files synchronized with each other and the project as a whole. This configuration management process applies to all files (Word, Excel, PowerPoint, Project, etc.) created as a part of the project, whether as a deliverable to be given to the client or as an internal project working paper. COTS development software (including web server and app server tools) is under the CM control of our Enterprise Technical Architecture group.

The goals are to:

- Have the ability to identify the most current copy of a particular document
- Have the ability to identify the who, when, and what for each document change

The project team will:

1. Store all electronic files in eProject under the TO 79 - Portals Rollout page (https://modpartner.eproject.com).
2. Only modify files which are within their responsibility

3. Record each document change in the edit history section
4. Preserve prior versions of DRAFT FINAL and FINAL electronic files by saving new versions of the file in the eProject Portals Rollout file repository

The standard naming convention for files in the eProject Portals Rollout file repository would include the following:

Description_date

The description of the file should convey (even to the uninitiated) the basic idea about what a given file is.

Naming standards for controlling versions is not necessary within eProject. As each document is checked out, eProject controls each version locally.

For example, a file containing the project workplan should be called:

"Portals Workplan_0808"

as opposed to:

"Portals WP_0808"

The format of the date as represented in the file's name should be in the following format: _mmddyy

Configuration management activities will include several areas of the development process. Configuration items are identified and version control procedures established and followed. Code is checked in and out through the configuration management tool Microsoft Visual SourceSafe. A standard directory structure within the development repository has been established for the Portals Rollout project. These guidelines ensure development processes continue efficiently and effectively. All changes must be controlled to ensure accurate tracking.

1.3.2 Configuration Identification

Configuration identification is the process for selecting, identifying, and naming configuration items. A configuration item is a file or a block of code that relates to a bug fix or a modification request that is managed as a single item and falls under configuration management. Some items are initiated and operated independently of the items; others are dependent and perform functions that satisfy end-user requirements.

Compiled code shall not be versioned by Microsoft Visual SourceSafe. This is done to limit the size of the repository. Source code will be controlled through Microsoft Visual SourceSafe.

Naming standards for controlling versions is not necessary within Microsoft Visual SourceSafe. As each document is checked out, each version is controlled locally by Microsoft Visual SourceSafe.

Prior to utilizing Microsoft Visual SourceSafe as the main configuration management tool the CM process for developing and migrating code will be a manual process. This process is documented in the Configuration Control section of this document

1.3.3 Change Control Process

During the development and maintenance processes, controlled baselines will change and configuration control is designed to manage the changes. Changes may be needed for a variety of reasons, such as adding new technology or functionality, correcting problems, and responding to technical and operational tests and evaluations. The Change Control Board is in place to review a change requests impact on performance, functionality, schedule, overall configuration/ architecture and budget. The overall change process for the Portals Rollout project is illustrated in the following diagram. This process will be closely followed throughout the testing cycle.

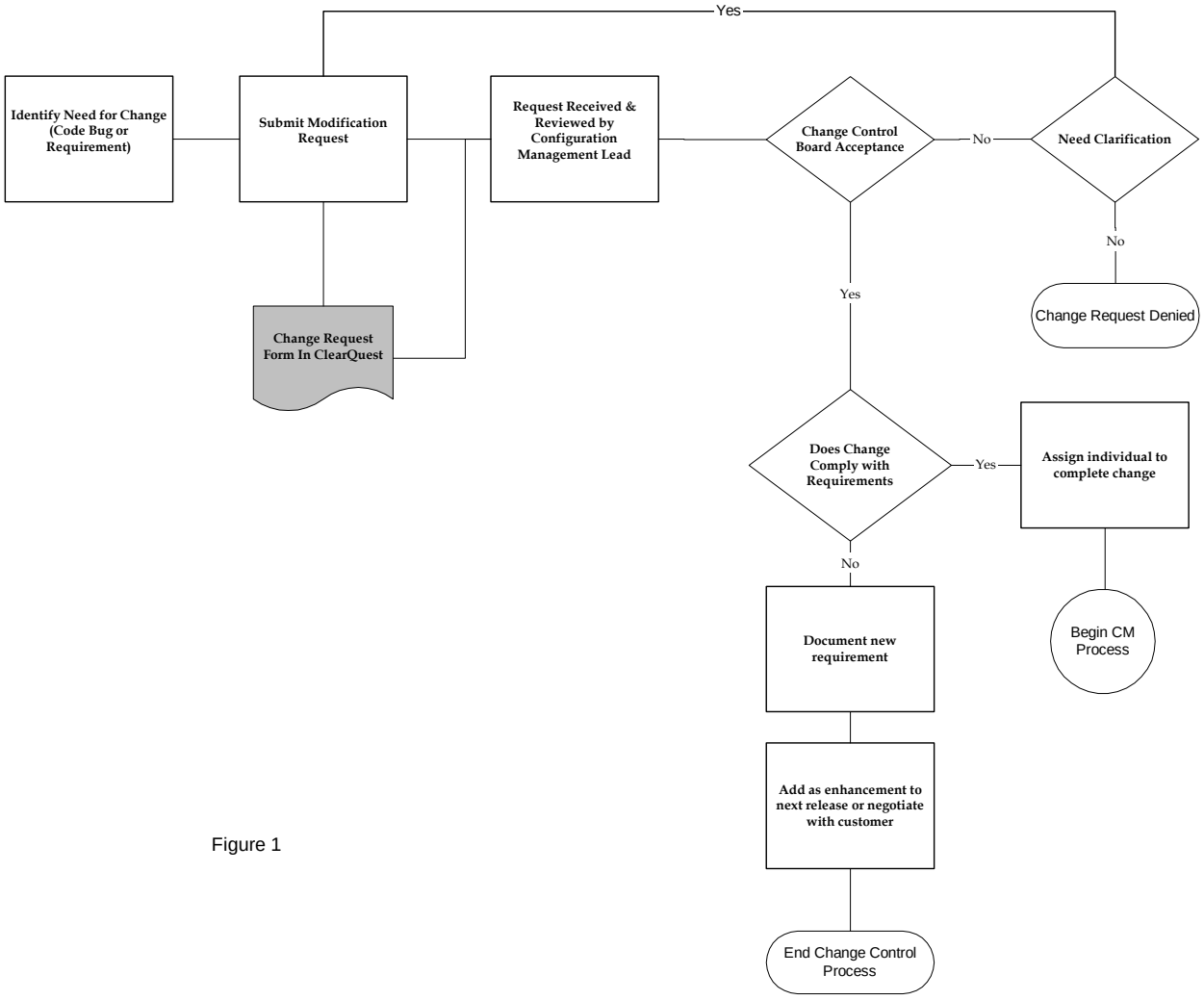

Figure 1

1.3.4 CM Tools

Rational's Microsoft Visual SourceSafe and ClearQuest will be utilized in order to facilitate the code migration, change requests, and error tracking.

In terms of tracking CM changes, the following procedures generally apply:

Step 1	A team member identifies a potential change that would impact a file, development object, or environment component.
Step 2	A Team Lead is notified of the potential change and evaluates the CM Change Request to determine if it is a Configuration or Scope Change Request. If it is a Configuration Change Request, the Team Lead has approval authority. If it is a Scope Change Request, the Scope Management process outlined in the Scope Management Plan is followed.
Step 3	The CM Change Requests created through the resolution of documented issues, or non-scope related problems discovered after initial configuration item signoff, are reviewed by Team Lead.
Step 4	All CM Change Requests will be logged in the appropriate Configuration Management tracking tool. Configuration changes, application updates, and environment changes will be logged in the Configuration Management tracking tool. Electronic file change requests will be tracked via the Documentation Control Log.
Step 5	The Team Project Manager updates the workplan to reflect the Change Request.
Step 6	The Team Lead makes the changes to the impacted configuration item(s) or delegates that responsibility to the appropriate person. The previous version of the impacted configuration item is stored in the CM tool for the duration of Portals Release 1 and Portals Release 2. At the conclusion of Portals Release 2 it will be up to the discretion of the client to determine how, and for how long, the configuration items are stored.
Step 7	The Team Lead communicates the impact of the approved CM Change Request to the affected parties.
Step 8	The Documentation Log is updated and the CM Change Control process is complete.

Configuration Management status is reported through the use of Document Control Logs and version history reports generated from our CM tool.

1.3.5 Configuration Control

Configuration control is the process of controlling change to the developed application. Configuration control includes the systematic evaluation, coordination, and approval of proposed changes to configuration items. In addition, configuration control also includes the process of moving developed source code from one environment to another at the proper times.

The migration plan below in figure 1 shows the relationship between the code migration, the environments, the testing that will be happening in each phase and environment, and the change management tools being utilized for this project.

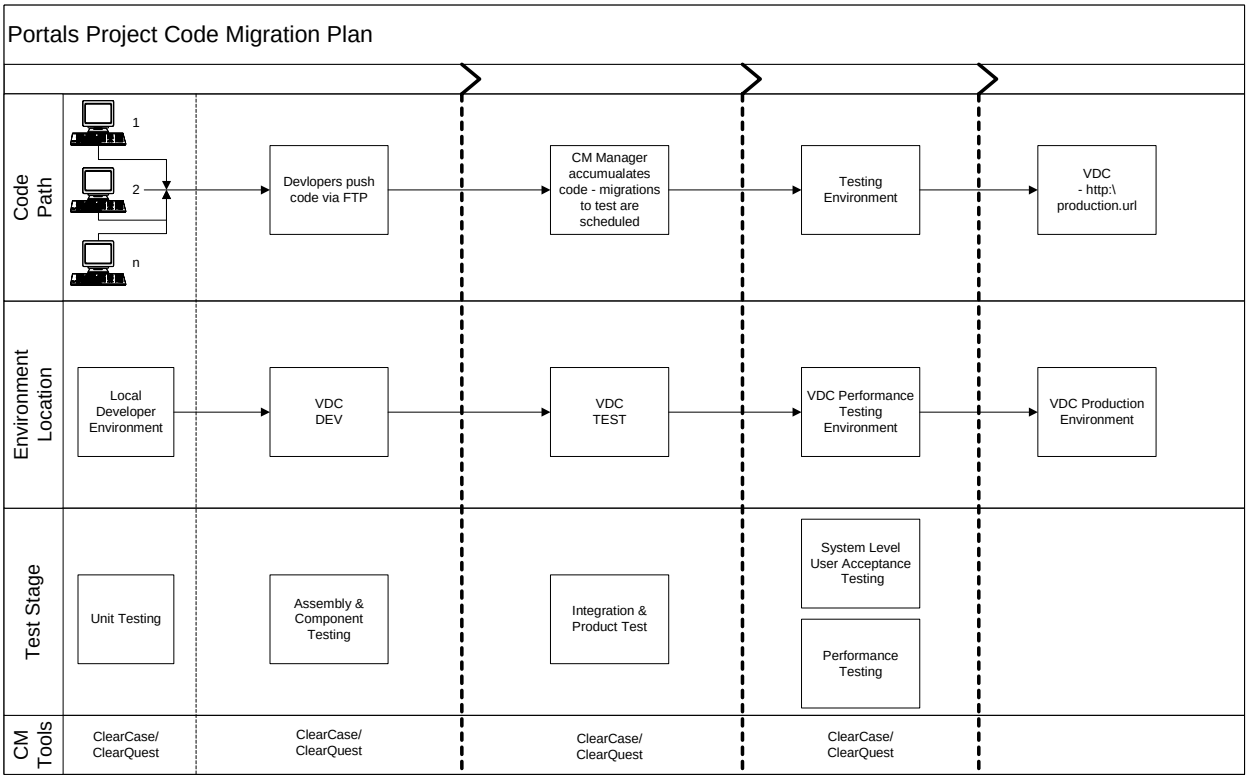

Figure 1

A tester or requestor must complete a change request to identify the reported problem and identify what requirement it is related to. All requests will be assigned a priority and then assigned to the appropriate party for resolution of the issue. Once the code is changed, it will be appropriately tested in the development and through all cycles preceding the point where the problem was found.

The tool being utilized for change control is Rational ClearQuest. The Change Control Lead and Iteration Test Manager will closely monitor the ClearQuest repository.

The code path (figure 1) is further defined in figure 2 below. The development of new software or changes to existing software based on the next iteration's design will follow the code path procedure shown in figure 2. It is the responsibility of the Configuration Management Lead to not only follow the procedure himself but to also verify that the developers are also adhering to the standards and processes that were put in place. The configuration manager maintains a list of code development called the Release Document. An example of this document is located in appendix A. This document is used by the Configuration Management Lead to track the code development of each developer. The code development will relate directly to a technical specification document, located in the detailed design documents, that was used by the developer as a "roadmap" to create a specific piece of the application. Each technical specification document was created in response to a requirement from the requirements document baselined and approved in the Vision Phase. All recorded requirements will be matched with application functionality to ensure expectations were met.

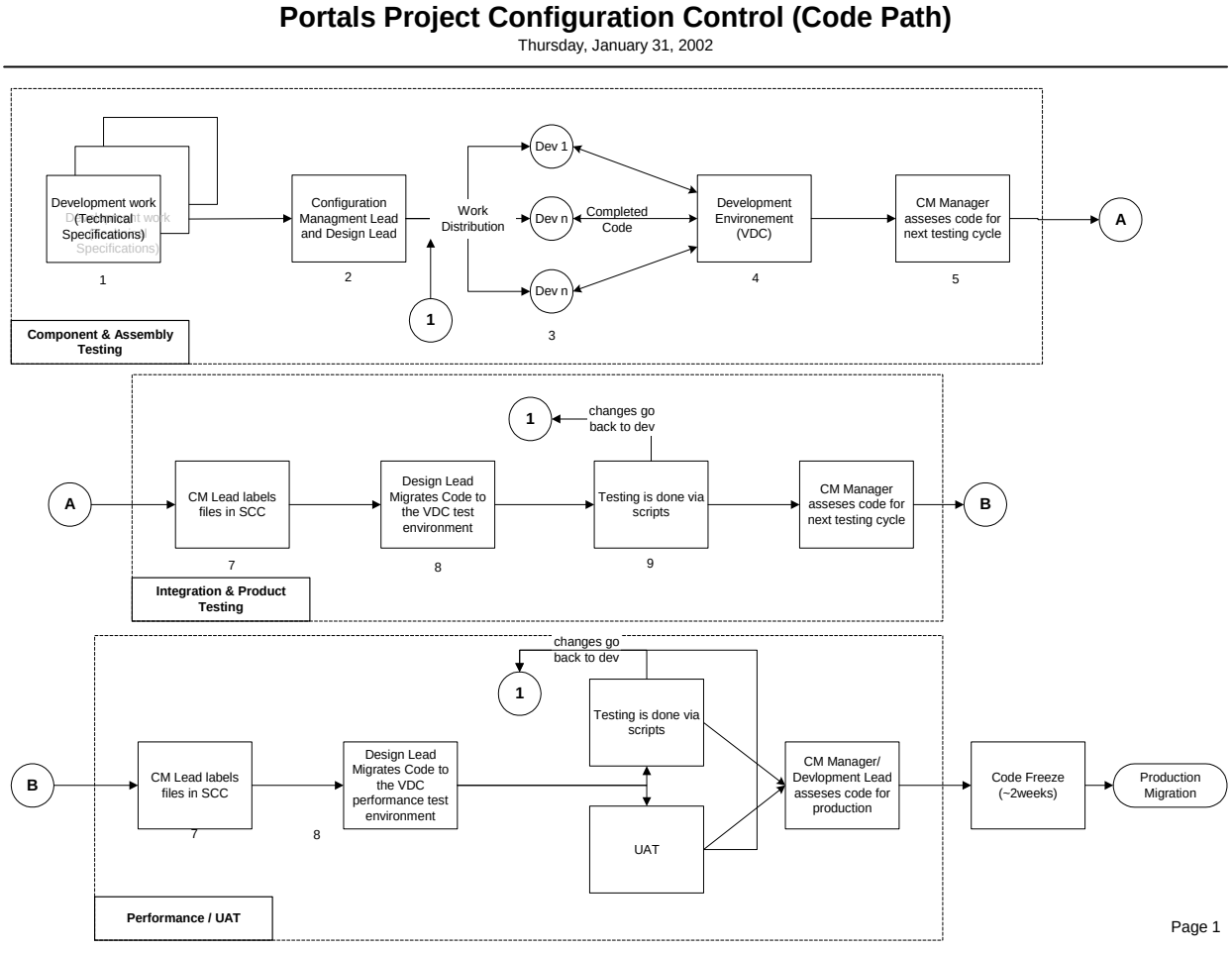

Figure 2

1.3.6 Configuration Baseline Auditing

At a minimum, audits should be performed between project phases. Therefore, an audit should be conducted before the project proceeds with the vision, definition, construction, deployment, and support phases.

1.3.7 Baseline Management

Baselining is the core of configuration management. By baselining, the Portals Rollout Team controls and measures the changes that occur to its configuration items in a given period of time and ensures the integrity of the product that is released. The CM lead, with input from the development team, will be responsible for performing the configuration baseline between project phases.

The table that follows identifies the configuration management processes that must be followed for each configuration item type. The following configuration management processes are discussed for each item type:

- Signoff – Specified items must be formally reviewed and signed-off by designated project participants.
- Configuration Change Control – All changes to specified items must be requested and approved before the change can be implemented. Change control will formally begin after the initial signoff of (i.e., changes made before the initial signoff do not require formal approval).
- Version Control – All modifications to specified items must be documented by either incrementing the version number for the items or by providing comments that list the chronology and description(s) of the change(s). Version control will formally begin after the initial signoff (i.e., changes made before the initial signoff do not require incrementing of the version number or addition of "versioning" comments).
- Migration Control – Movement of software objects or data from one environment to another must be formally requested and approved before the migration can be implemented. In general, this process is not applicable to design and development documentation.
- Access Control – Access to specified items will be controlled. Only project team members with access rights will be able to make changes to these items.

Item Category	Item Type	Signoff	Change Control	Version Control	Migration Control	Access Control*
Project Plan	Work Plan	Yes	Note 1	Yes	No	B
	Work Estimate	Yes	Note 1	Yes	No	B
Data	Master and Configuration Data	Yes	Yes	No	Yes	W
Vision	Requirements/Item Tracking Log	Yes	Yes	Note 4	No	B
	General Design Specification	Yes	Yes	Yes	No	B
Other	Problem Tracking (SIR) Log	No	Note 2	Note 4	No	B
	Change	Yes	N/A	Note 4	No	B

Item Category	Item Type	Signoff	Change Control	Version Control	Migration Control	Access Control*
	Request Log					

*Access Control – Read (R), Write (W), Both (B), Neither (N)

Note 1 – Changes to the Work Plan and Work Estimate occur as a result of the Change Control process. When a change request is evaluated, an estimate of the work will occur. The estimate will be used in the evaluation process. If the Change Request is formally approved, appropriate changes will be made to the Work Plan and overall Work Estimate.

Note 2 – The Issues Log and Problem Tracking log are not subject to the Change Control process per se. However, Issues and Problems (SIRs) may get elevated to Change Request status.

1.3.8 Configuration Items

The following Items are to be subjected to the configuration management practices set forth in this plan:

- Project Management Items:
  - Project Plan
  - Solution Acquisition Plan
  - High Level Requirements
  - Security Vision Phase Checklist
  - Quality Assurance Plan
  - Configuration Management Plan
  - Security Assignment Letters
  - Detailed Requirements Document for FP & Students
  - Requirements Traceability Matrix
  - Preliminary Design Document
  - Weekly/Biweekly Status reports
  - Master Point of Contact List
  - All Project Procedures, Policies, and Standards

- Development Items
  - JSP Pages
  - HTML Pages
  - Servlets
  - Java Beans

- COTS and associated configuration files and patches

1.4 Audits and Reports

1.4.1 Configuration Management Audit Process

Configuration management audits will be conducted on the 15th of every month. The audit process will consist of a designated person from the Quality & Process Improvement team who will maintain a spreadsheet which tracks existing configuration management realities against the established baselines. The auditor will periodically examine and update the spreadsheet:

- Auditor will create a new audit worksheet by copying the last audit worksheet. If any CM issues are identified, the document owner will be notified of the issue. The document owner will be responsible for updating the Control Log with the appropriate documentation to justify the updates and communicating the actions taken to the Configuration Manager. The auditor will then update the Configuration Management Plan audit worksheet with the date/action taken.
- The Technical Team will conduct monthly Configuration Management Audits for electronic files.

1.4.2 Configuration Management Metrics Tracking

The configuration management metrics tracking process will track the following metrics and create a monthly report:

- Total number of changes for all environments
- How many changes were disapproved
- How many changes are currently open
- How many have been opened since the last report
- How many have been closed since the last report

1.4.3 Audit Schedule

Name of CM activity (Report, Audit, etc.)	SDLC Phase	Scheduled completion date
N/A	Vision	N/A
		N/A
N/A	Definition	N/A
		N/A
Audit	Construction	N/A
Report		N/A
Audit	Deployment	9/15
Report		9/20
Audit	Support	10/15
Report		10/20

Appendix A – Release Document

"Release Document.xls"